TXOne Networks

2021

/Q3

Defending Railway Operations

from Targeted Cyberattacks

txOne networks

TXOne Networks

Defending Railway Operations

from Targeted Cyberattacks

txOne networks

▲ *The city's railways are appealing targets for the fast-changing forms of attack constantly under development by dedicated cyber-attackers*

Executive **Summary**

A city's rails make up its vital system, its veins and arteries. In Tokyo's Shinjuku station, trains pass through every few seconds that will carry more than 3.5 million people[1] each day. Disruption of a nation's railways is also disruption of its society, economy, and culture.

Attacks on railways used to come solely from outside cyberspace. Posters in train stations warn passengers to look out for suspicious behavior or abandoned luggage, and guards walk the stations ready to protect the public. However, in today's world, bad actors in criminal organizations or the employ of state governments much prefer to conduct their attacks over the internet from the comfort of their computer chairs.

This state of affairs makes cyberattackers much more challenging to apprehend and creates a need for cutting-edge defenses that can be rapidly and conveniently integrated into routine railway operations. These defenses must be resource-friendly and transmit data quickly enough to keep up with the transport of commuters and to accommodate the distributed nature of modern railway technologies, which distribute computation to provide comfort, safety, and speed to commuters and personnel. Securing daily operations and caring for passengers' trust means protecting computation from disruption while maintaining maximum availability, with no aspects of the exchange using more time or resources than necessary.

[1] Nippon.com, "Shinjuku Station is Enormous! Daily Passengers Equivalent to Population of Yokohama", Aug 31 2018

Threats to the **Ever-Moving Architecture of Railway Assets**

Mass Transit magazine writes about how, at the 2015 CeBIT Hannover Fair, security specialists created a realistic simulated rail network, which they put online to see how much attention it would get from hackers. It was complete with fake "CCTV feeds, control interfaces, train schedules, and running time status updates". Over its 6-week runtime, 2,745,267 cyberattacks were documented, and in "about 10 percent of the attacks" intruders were able to gain some control over simulated assets. Attackers would come back again and again, studying the system intensely and gaining more access every time – if the honeypot had run for a longer time, it's likely that these intruders would have found their way to escalated privileges within the railway system, and the ability to cause significant disruption. [2]

The distributed network architecture of railway infrastructure allows incredible adaptability and for the use of a wide variety of modular assets. It's likely to include long-lived legacy controllers or equipment that are essential to operations – often the most vulnerable assets in a system. In contrast, the fast-paced development of new forms of attack guarantees that the threat landscape can change completely in a matter of weeks.

The fast-changing nature of cyber threats runs up against the long service life and diversity of equipment, making the enforcement of security policy daunting. The large community of suppliers and the extended life cycles of railway assets create convenience and reliability in the physical world, while in cyberspace creating potential for catastrophic disruption due to compatibility issues, diverse patches and maintenance procedures, and vulnerabilities in assets that are no longer patchable. This is why specially designed cybersecurity appliances and software can be so essential to their safekeeping. Safety systems are one of the likeliest targets for attack, as they give the attacker immediate leverage over stakeholders.

[2] Vlad Gostomelsky, "Securing the Railroads from Cyberattacks", Mass Transit Magazine, Dec 17 2019

TXOne's transportation technology experts describe rail as "a system of systems", because the support of many subsystems is necessary for rail systems to run safely or often to run at all. Daily operations, maintenance, and public safety are all performed and maintained by these subsystems. While several subsystems are dedicated to the crucial task of functional safety, other subsystems in stations or rolling stock are also very appealing targets to cybercriminals. Attackers will seek to redirect trains as in the 2008 case in Poland,[3] or might shut down ticket sales and demand a steep ransom for their return as in the attack on the San Francisco Municipal Transportation Agency in 2016.[4] Hackers will leverage whatever privileges they can acquire, maximizing disruption.

The Train Control and Management System (TCMS) comes in a variety of architectures that all require access to a tremendous amount of widespread information as well as the ability to send out rapidfire commands, detecting equipment failure and resolving the resultant issues before they become problems. Similarly, the supervisory SCADA or, in some cases, DCS must extend its reach to every station, and systems aboard carriages or deployed at the wayside are often networked into a "ring" or "chain"-like architecture to increase redundancy and maximize connectivity, allowing for the viability of functions like the carriage's safety integrity level (SIL). Delivering safety reports and other data to the authorities, providing automatic updates of train schedules and real-time locations, and transmission of the telematics necessary for predictive maintenance are just a few of the routines for which modern transportation relies on high connectivity.

The same high-connectivity pathways that increase accessibility for trusted railway technicians also increase accessibility for malicious intruders. A successfully exploited vulnerability in any one of these increasingly interwoven and layered technologies has the potential to lock up operations on a large scale, and as they gain complexity they only become more challenging to secure.

Modern cyber attacks are more often than not based on using stolen credentials to take advantage of privilege hierarchies that are already in place, as in the 2015 case in South Korea when

▲ *As the railway industry has modernized and become increasingly automated, cyber-threats have increased in potential for catastrophe*

cybercriminals alleged to be in the employ of the North Korean government stole data from personal smartphones. South Korea's National Intelligence Service (NIS) was called into action to control the incident, fortunately before stolen credentials could be used to cause harm. They later released a statement that it is necessary to prepare for a coming increase in "cyber terror against the railway transport control system".

[3] Chuck Squatriglia, "Polish Teen Hacks His City's Trams, Chaos Ensues", Wired Magazine, January 11 2008

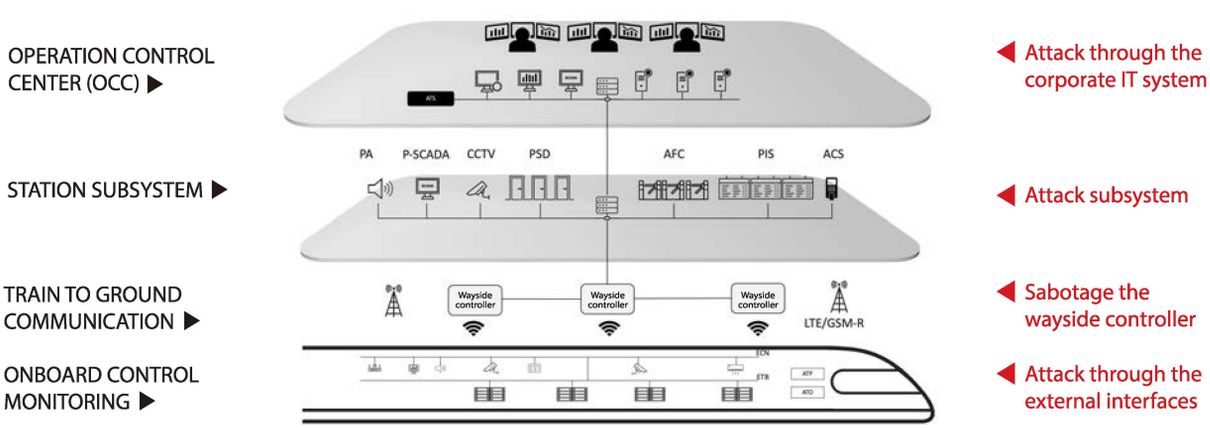
[4] Jim Finkle, "San Francisco public transit system hit in ransomware attack", Reuters, Nov 28 2016

Attacks in 2020 showed clearly the immense potential for catastrophe that hackers can inflict on modern transportation technology. In July, a group of hackers calling themselves "Cyber Avengers" attacked Israel's railway infrastructure. The attackers claimed that their attacks, continuing for ten days, disrupted operations at 28 railway stations and caused "severe damage to equipment and infrastructure", though these claims were unconfirmed by Israeli's railway operators. They stated that the attack was intended to show the hackers' ability to cause tens of trains to collide. Like this case, many cyber attacks in recent years have had claims or evidence attached that suggested them to be acts of terrorism.

Most recently, on July 20th of 2021, touchscreen ticket machines used by England's Northern Rail company were taken completely offline by ransomware.[5] According to ZDnet the attack hit just two months after Northern Rail deployed 600 of the machines at 420 different stations, forcing sales to be conducted through the mobile app, website, and ticketing personnel. Cybersecurity specialists at SecurityWeek have speculated that this attack was not targeted and was instead the result of 'spray and pray' tactics, which focus on disseminating ransomware at high volume and attacking opportunistically instead of tailoring attacks to specific organizations or fields.[6] Incidents like this one will become less common as railway organizations continue to adopt more rigorous cybersecurity standards.

Communications-Based Train Control (CBTC)

- SCADA
- HMI
- Data Servers
- Automatic Train Supervision (ATS)
- Public Address (PA)
- Power SCADA
- CCTV Surveillance
- Platform Screen Door System (PSD)
- Automated Fare Collection (AFC)
- Passenger Information System (PIS)
- Access Control System (ACS)
- Ethernet Consist Networks (ECN)
- Ethernet Train Backbone (ETB)
- Automatic Train Protection (ATP)
- Automatic Train Operation (ATO)



[5] Danny Palmer, "Hundreds of touchscreen ticket machines are offline after a ransomware attack", ZDnet, July 20 2021
[6] Kevin Townsend, "Ransomware Attack on UK Rail System Spray and Pray or Targeted?", SecurityWeek, July 21 2021

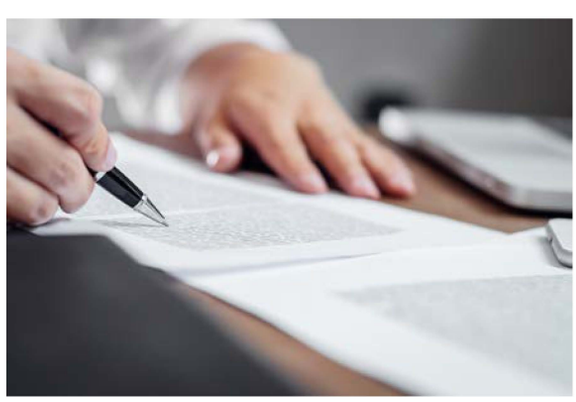
The Regulations Make the Terrain

Each of the rail subsystems is a totally different set of equipment, each covered by its own department of operators who are running different technologies with different cybersecurity needs. For this reason many of these have their own unique security standards to which they must adhere – the CCTV and signaling subsystems, for example, have different functionalities, authentications, and disciplinary backgrounds for their technicians.

The safety-classified railway applications necessary to each subsystem have all been systematically type-tested and secured according to relevant certifications prior to leaving the factory. In other words, they're intended to be secure by design. While this brings with it a multitude of benefits, the drawback of certifications is that they introduce common patterns into defenses that hackers can learn to predict and work with.

If a cybercriminal can identify a vulnerability in one asset, that same vulnerability is likely to exist in other assets following the same certifications. In short, cybersecurity and compliance have an important relationship but are not the same. Solutions must be made available that go above and beyond safety certification and which have the constant support of dedicated security intelligence researchers so that they can pivot to address new cyber threats.

Drawing influence from many existing regulations such as IEC 62443, EN 50126, and CSM-RA, CENELEC's new TS 50701 standards are projected to be available by summer of 2021 and will go a long way towards improving the cybersecurity of railway operations.[7] They're designed to consider rail as an ecosystem (of which the train itself is one of many parts), to address the ease of access that malicious actors have to physical systems, and to classify systems as "safety-critical" or "non safety-critical". These new regulations improve synchronization between stakeholders, create an overall rise in safety and security, and promote commercially viable cybersecurity for vendors, manufacturers, and operators. Technicians will need to be prepared to integrate cybersecurity into every phase of the asset life cycle, with special attention to the legacy systems that are common in the railway environment.



▲ *These same regulations that create protections also create patterns in cyber defenses that attackers can learn to predict*

[7] ENISA-ERA Conference: Cybersecurity in Railways, "CENELECprTS 50701", Mar 16 2021

Leading Edge Solutions for Legacy & Modern Railway Assets

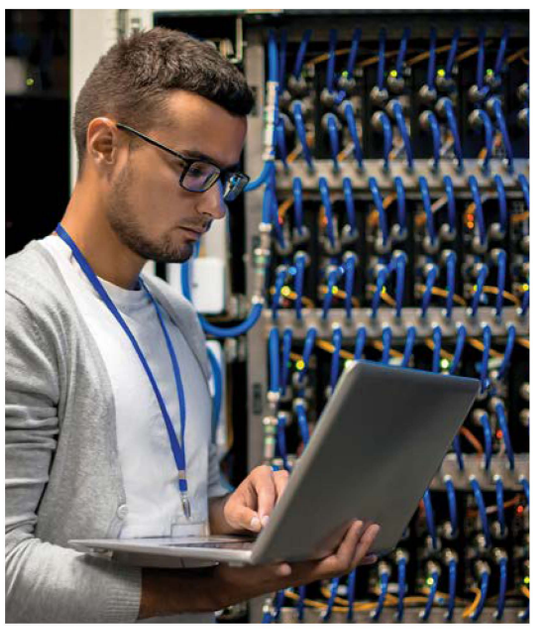
While it's often said that cybersecurity begins with education, the busy day-to-day work of railway personnel rarely leaves a surplus of extra time, and so all defensive solutions must be as failsafe and streamlined as possible to promote ease of use. Ideally, an appliance should be deployed that has the necessary protocol sensitivity to check network traffic for suspicious actions and deny unusual or unlikely behavior. Such appliances have the added benefit of significantly reducing the likelihood of human error.

Modular assets like TCMS require spread out solutions so that every part of the system is protected. Every unique subsystem must be set up with solutions designed around its specific needs – fixed-use endpoints with lockdown software, modern endpoints with lightweight next-generation antivirus, mobile assets with portable rapid-scan technology, and networks with the OT security triad of segmentation, inspection, and virtual patching. Maintaining the constant operation of railway systems requires protection from the threats of today as well as tomorrow. As the critical industry of railways continues to grow, so too will cyber attacks against it.

▲ *Vulnerabilities and specialized maintenance procedures both increase in number as legacy and modern assets run side-by-side*

Halting Intrusions and Isolating Malware

Intrusion prevention systems (IPSes) were once mere filtering systems, and such IPSes are no longer adequate protection for critical infrastructure networks. Appliances in our Edge series bring more sophisticated protection to assets at the station and wayside, including both next-generation IPSes and a next-generation firewall. This family of solutions detects suspicious behavior on legitimate accounts or from legitimate devices, puts a virtual patching "shield bubble" around legacy assets that can't be patched or replaced, and segments networks so that they're much more defensible.



▼ *Distributed railway access points require solutions that are easily deployed in a range of locations*

EdgeIPS technology is available in two forms – regular EdgeIPS, which is designed for micro-segmentation on a 1-to-1 basis, and EdgeIPS Pro, the industrial IPS array, which provides east-west cross-zone protection for 24 or 48 segments from a single centralized location. In the station, EdgeIPS Pro works best deployed directly beneath the station's rack-mounted ethernet switch, where it can inspect all traffic in and out of the station subnet with superior protocol sensitivity. Its minimized latency keeps data transmission optimally quick as it's secured.

The access points (APs) that a train uses for mesh or roaming are often running with limited or hardly any security. Ordinarily, if someone stands in the wayside and takes out their smartphone, they can find an AP's access ID and attempt to gain entry, and having done that will be able to affect the signal control system. EdgeIPS is perfect for deployment between the AP and its switch, preventing it from being compromised.

The wayside's safety- and mission-critical circuit monitoring, signal control, detection, and point machine assets all benefit from EdgeIPS security boxes running on a 1-to-1 basis, preventing interference by malicious actors. EdgeIPS' ruggedization is perfect for maintaining a high mean time between failure even in the potentially harsh environments of the wayside, where equipment cabinets can be exposed to extreme temperatures for extended periods of time. If an AP requires multiple ports, another device in the Edge family, the next-generation firewall EdgeFire, makes an effective bridge. One of its multiple ports serves for the AP, while the others are for control devices and the link to the switch.

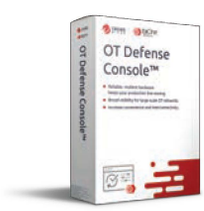
One common sign of malware infection is suspicious outbound traffic resulting from the unwanted application trying to "phone home" or spread itself around the network, which Edge series nodes detect and stop. While modern cyber attacks are commonly based on stolen credentials, EdgeIPS series nodes have the ability to detect unusual traffic even among apparently approved devices or accounts, minimizing the potential for human error as well as stopping intruders from sending out commands on the network. It does this via a trust list, which functions by specifying approved commands and connections.

ICS Network Defense

TXOne EdgeIPS™
Micro-segmentation by customizable zone

TXOne EdgeIPS™ Pro
Purpose-built industrial IPS array

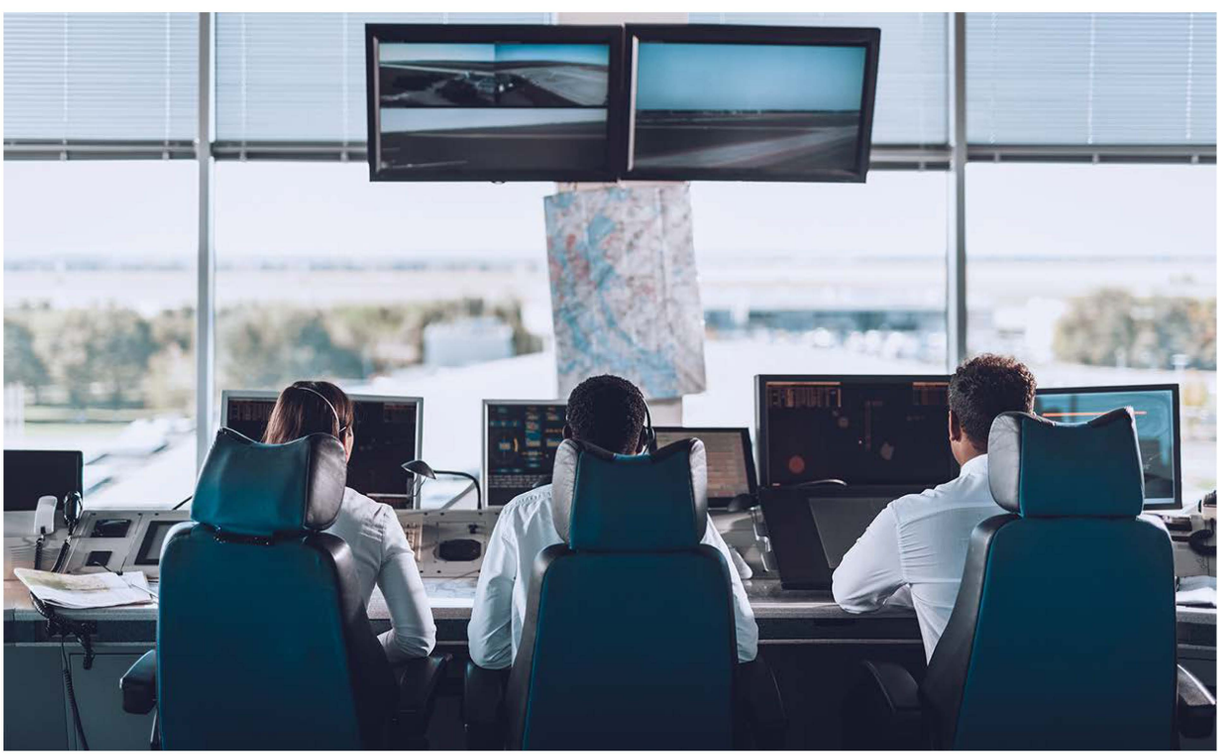
TXOne EdgeFire™
Internal segmentation with intention-based zoning



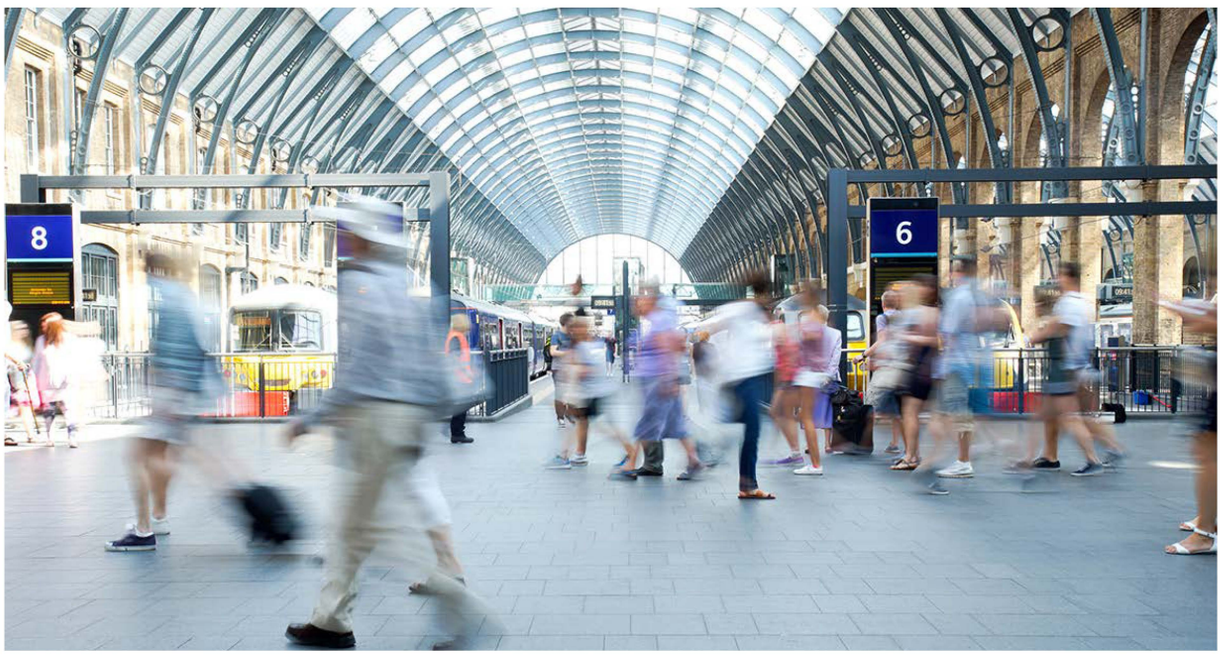
OT Defense Console™ (ODC)
ICS network security management

In rail, where gear as old as 20 years may still be in use, legacy assets benefit from special protections operating efficiently from the network without requiring any modification to the device. Virtual patching, which is supported by TXOne Networks' team of security intelligence specialists, is a network-based technology that shields the vulnerabilities of legacy assets while supporting their maximized availability and operation. This technology was specifically created to address the needs of mission-critical assets well-past their end-of-service (EOS) date.

TXOne Networks recommends network segmentation to be built into network architecture from the ground up, as it substantially increases visibility while allowing the system much more defensible against cyber attack. Segments in a network are created based on "intentionality", or which assets or subsystems must communicate to do their work. EdgeIPS technology can segment the network at the time it's transparently deployed, requiring no changes to existing architecture while increasing security considerably. Malicious behavior is much easier to detect when it's visible as unusual movement between segments. To better support railway control systems operating from differing geographic locations, Edge series deployments can be centrally managed via integration with OT Defense Console.



▲ *Mobile and stand-alone OT assets benefit from portable solutions that support high availability*



For Mobile and Stand-Alone Assets

Platform screen door control systems, fare collection and speed gate systems, depot assets, ventilation systems, train-borne equipment, PA systems, and surveillance systems have all been successfully scanned with Trend Micro Portable Security 3 (TMPS3). This is a USB stick-based technology that fits easily in the palm of your hand, and which is designed for easy use even by personnel without formal technical training. Status is indicated by three lights on its body – blue for no malware detected, green for malware detected and removed, and red for malware detected with further action required.

Devices brought on-site by vendors or maintenance experts are one of the most common ways dangerous threats are introduced to the OT network. In addition to routine scans of deployed technology, our security intelligence specialists recommend using TMPS3 for pre-scans of new equipment prior to its deployment on the network and for setting up a checkpoint to scan all laptops and other devices that are brought on-site by maintenance staff. TMPS3's ability to conduct quick scans without installing any software makes it perfect for checkpoint scans as well as sensitive equipment that can't accept installation or modification.

Trend Micro Portable Security™ 3 ▼

Installation-free endpoint security inspection

▲ *The anatomy of rolling stock is made up of many onboard systems that require individualized awareness in security posture*

For Fixed-Use and Legacy Assets

For fixed-use assets like ticketing stations and on-board computers, StellarEnforce is the ideal solution. Even if malware finds its way into your working hardware, it's unable to execute due to StellarEnforce's trust list-based 4-in-1 lockdown. Applications, configurations, data, and USB devices are all locked down with a trust list that excludes all applications that are unlisted from executing and all users that are unlisted from making changes to data or configurations. Only administrator-approved USB devices can connect to the device, and only an administrator can grant a device 1-time approval to connect.

StellarEnforce is already in use within many transportation OT networks. Our security intelligence specialists recommend its use for fare collection systems, speed gates, telephone control systems, CCTV surveillance systems, passenger information system (PIS) computers, and PA systems.

▲ *Locking down fixed-use assets streamlines their security, simplifying maintenance*

▲ TXOne Stellar™ Series
ICS Endpoint Protection

www.txone-networks.com
support@txone-networks.com


txOne
networks